CLAIMS:

1. A system comprising a trusted computing platform, one or more logically protected computing environments and a filesystem comprising a plurality of files and links defining access paths between said files, the system being arranged to load onto said trusted computing platform a predetermined security policy including a plurality of security rules in respect of one or more of said logically protected computing environments and/or said files, the system being further arranged to determine that first and second security rules apply to a specified file or set of files, determine the complete set of files (or fileset) to which each of said first and second security rules applies, determine if the fileset of said first security rule is a complete subset of the fileset of said second security rule, and if so, apply said first security rule to said specified file or set of files, and otherwise, select one of said first and second security rules on the basis of another attribute thereof, and apply the selected security rule to said specified file or set of files.

2. A system according to claim 1, wherein said security rules comprise or include a plurality of file rules defining discretionary access controls in respect of one or more of said logically protected computing environments and/or files.

3. A system according to claim 1 or claim 2, wherein said security rules comprise or include a plurality of execution control rules defining a modifying security attributes in respect of one or more of said logically protected computing environments and/or files.

4. A system according to claim 2, wherein in said first and second security rules are file rules, and the fileset to which said first security rule applies is not a complete subset of the fileset to which the second security rules applies, the system is arranged to determine which of the first and second security rules is the most restrictive, and apply that rule to said specified file or set of files.

5. A system according to claim 3, wherein if said first and second security rules are execution control rules and the fileset to which said first security rule applies is not a complete subset of the fileset to which said second security rule applies, the system is arranged to select and apply the rule which was most recently added to the security policy.

6. A system according to claim 5, arranged to provide a warning or error message indicating to a user that a rule conflict exists.

7. A system according to any one of the preceding claims, including means for identifying the creation of a rule conflict when a link between files or sets of files is created and providing an error message or warning accordingly.

8. A system according to claim 7, arranged to remove the offending link to remove the conflict.

9. A system substantially as herein described with reference to the accompanying drawings.

10. A method of applying a predetermined security policy to a system having trusted computing platform, one or more logically protected computing environments and a filesystem comprising a plurality of files and links defining access paths between said files, said security policy including a plurality of security rules in respect of one or more of logically protected computing environments and/or said files, the method comprising the steps of determining that first and second security rules apply to a specified file or set of files, determining the complete set of files (or fileset) to which each of said first and second security rules applies, determining if the fileset of said first security rule is a complete subset of the fileset of said second security rule, and if so, applying said first security rule to said specified file or set of files, and otherwise, selecting one of said first and second security rules on the basis of another attribute thereof, and applying the selected security rule to said specified file or set of files.

11. A method according to claim 10 wherein the security rules define access controls and/or modify security attributes.

12. A method of applying a predetermined security policy to a trusted computing platform, the method being substantially as herein described with reference to the accompanying drawings.